AMENDMENTS TO THE CLAIMS

The claims in this listing will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A device authentication system in which a first device authenticates a second device, the second device not having a secure area,

wherein the first device comprises:

a transmission/reception section that transmits and receives information to/from the second device;

a first information holding section that holds first authentication information in a secure area; and

a decider that makes a decision on authentication,

the second device comprises:

a transmission/reception section that transmits and receives information to/from the first device;

a second information holding section that holds second authentication information;

an information acquirer that acquires third authentication information from externally of the second device, said third authentication information comprising ~~user identification information~~ secret information input by a user; and

an authentication information generator which generates fourth authentication information from the second authentication information and the third authentication information, and outputs the fourth authentication information to the first device through the transmission/reception section,

wherein the decider makes a decision on conformity between the first authentication information and the fourth authentication information to authenticate the second device, and

wherein, when the first device does not hold the first authentication information, a device that performs mutual authentication with the first device acquires the fourth authentication information from the second device, and sets the first device for the first authentication information as an initial setting.

2. (Original) The device authentication system according to claim 1, wherein the second authentication information is information specific to the second device.

3. (Original) The device authentication system according to claim 1, wherein the second authentication information is random information generated in the first device.

4. (Previously Presented) The device authentication system according to claim 3, wherein the second authentication information is updated whenever the authentication processing is performed, and in accordance with the update of the second authentication information, the first authentication information held in the first information holding section in the first device is updated.

5. (Canceled)

6. (Previously Presented) The device authentication system according to claim 1, wherein the third authentication information is held in a predetermined device that performs mutual authentication with the first device, and is provided from the predetermined device to the second device in authentication processing.

7. (Currently Amended) A device authentication method in which a first device authenticates a second device, the second device not having a secure area, the method comprising:

holding, by the first device, first authentication information in a secure area,

holding by the second device, second authentication information, and generating fourth authentication information from the second authentication information and third authentication

information provided from externally of the second device, the third authentication information comprising ~~user identification information~~ secret information input by a user, and

deciding, by the first device, on conformity between the first authentication information and the fourth authentication information to authenticate the second device

wherein, when the first device does not hold the first authentication information, a device that performs mutual authentication with the first device acquires the fourth authentication information from the second device, and sets the first device for the first authentication information as an initial setting.

8. (Currently Amended) A second device to be authenticated by a first device that holds first authentication information in a secure area, the second device not having a secure area, the secured device comprising:

a transmission/reception section that transmits and receives information to/from the first device;

an information holding section that holds second authentication information;

an information acquirer that acquires third authentication information externally of the second device, the third authentication information comprising ~~user identification information~~ secret information input by a user; and

an authentication information generator which generates fourth authentication information from the second authentication information and the third authentication information, and outputs the fourth authentication information to the first device through the transmission/reception section

wherein, when the first device does not hold the first authentication information, a device that performs mutual authentication with the first device acquires the fourth authentication

information from the second device, and sets the first device for the first authentication information as an initial setting.

9. (Original) The second device according to claim 8, wherein the transmission/reception section receives random information from the first device, and the authentication information generator encrypts the random information using the fourth authentication information to transmit to the first device through the transmission/reception section.

10. (Previously Presented) The second device according to claim 8, wherein the transmission/reception section receives random information from the first device, and the authentication information generator encrypts the fourth authentication information using the random information to transmit to the first device through the transmission/reception section.

11. (Previously Presented) The second device according to claim 8, further comprising:

an update control section that controls updating of information required for authentication processing,

wherein after authentication from the first device succeeds, substituting for the second authentication information, the update control section stores, in the information holding section, the random information as new second authentication information, generates key information that is new authentication information from the third authentication information and the random information, and has the first device hold the key information through the transmission/reception section.

12. (Previously Presented) The second device according to claim 9, further comprising:

an update control section that controls updating of information required for authentication processing,

wherein after authentication from the first device succeeds, substituting for the second authentication information, the update control section stores, in the information holding section,

the random information as new second authentication information, generates key information that is new authentication information from the third authentication information and the random information, and has the first device hold the key information through the transmission/reception section.

13. (Previously Presented) The second device according to claim 10, further comprising:

an update control section that controls updating of information required for authentication processing,

wherein after authentication from the first device succeeds, substituting for the second authentication information, the update control section stores, in the information holding section, the random information as new second authentication information, generates key information that is new authentication information from the third authentication information and the random information, and has the first device hold the key information through the transmission/reception section.

14. (Currently Amended) A first device that authenticates a second device, the second device containing second authentication information and not having a secure area, acquiring third authentication information externally of the second device, the third authentication information comprising ~~user identification information~~ secret information input by a user, and generating fourth authentication information from the second and third authentication information, the first device comprising:

a transmission/reception section that transmits and receives information to/from the second device;

an information holding section that holds first authentication information in a secure area; and

a decider that makes a decision on conformity between the fourth authentication information received in the transmission/reception section and the first authentication information

wherein, when the first device does not hold the first authentication information, a device that performs mutual authentication with the first device acquires the fourth authentication information from the second device, and sets the first device for the first authentication information as an initial setting.

15. (Original) The first device according to claim 14, further comprising:

a random information generator that generates random information to transmit to the second device through the transmission/reception section,

wherein the decider decodes information received in the transmission/reception section using the first authentication information, and makes a decision on conformity between the decoded information and the random information.

16. (Original) The first device according to claim 14, further comprising:

a random information generator that generates random information to transmit to the second device through the transmission/reception section,

wherein the decider decodes information received in the transmission/reception section using the random information, and makes a decision on conformity between the decoded information and the first authentication information.

17. (Original) The first device according to claim 14,wherein after authentication of the second device succeeds, substituting for the first authentication information, the information holding section holds key information that is new authentication information received in the transmission/reception section, as new first authentication information.

18. (Original) The first device according to claim 15,wherein after authentication of the second device succeeds, substituting for the first authentication information, the information holding section holds key information that is new authentication information received in the transmission/reception section, as new first authentication information.

19. (Original) The first device according to claim 16,wherein after authentication of the second device succeeds, substituting for the first authentication information, the information holding section holds key information that is new authentication information received in the transmission/reception section, as new first authentication information.

20. (Currently Amended) A computer readable medium that stores a program for having a computer, which is integrated into a second device to be authenticated by a first device, perform the authentication, the second device not having a secure area, the computer readable medium:

a generating code segment that generates fourth authentication information from second authentication information that the second device holds and third authentication information acquired from externally of the second device the third authentication information comprising ~~user identification information~~ secret information input by a user;

a requesting code segment that requests issuance of random information to the first device; and

an encrypting code segment that encrypts the random information received from the first device using the fourth authentication information to output to the first device

wherein, when the first device does not hold the first authentication information, a device that performs mutual authentication with the first device acquires the fourth authentication information from the second device, and sets the first device for the first authentication information as an initial setting.